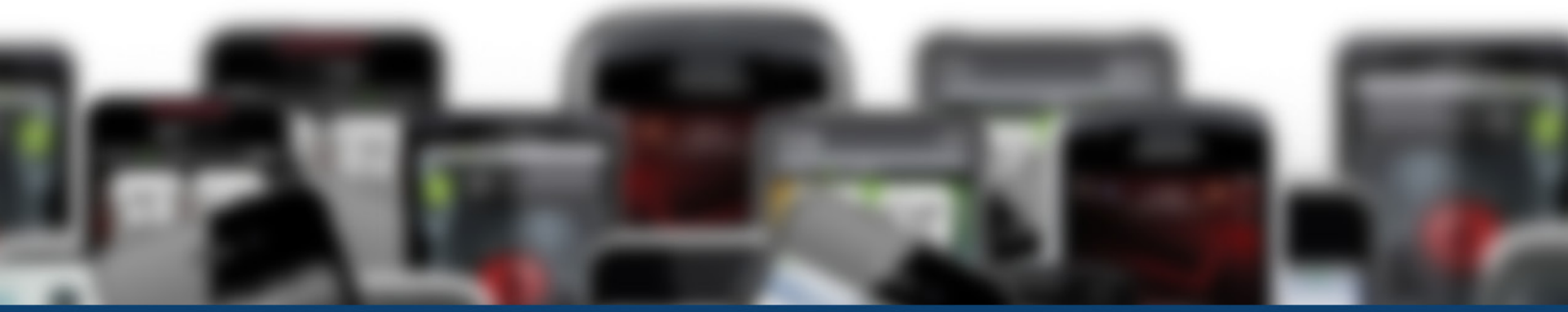


Do I Need BYOD?

The Rise of Bring Your Own Device Policies

TABLE OF CONTENTS

Do I Need BYOD?

INTRODUCTION

"Bring your own device" (BYOD) policies have existed since the advent of the web-enabled mobile phone. These policies have become much more commonplace in the wake of the ongoing boom in the smartphone market.

Presently, 80% of companies in North America support email, contacts, and calendar functions on mobile phones and tablets. Accordingly, it goes without saying that employees are accessing their corporate email and documents from devices that are not companyowned.

This consumerization of corporate IT means that employees are handling work functions from a larger range of devices. An Excel spreadsheet is no longer just seen on a Windows machine at the office; it might be edited on an iPhone and later sent to an accounting team working on Macs. Corporate IT can no longer assume that information and documents will be used on one kind of device using just one operating system; the device ecosystem is more diverse and varied than it has ever been.

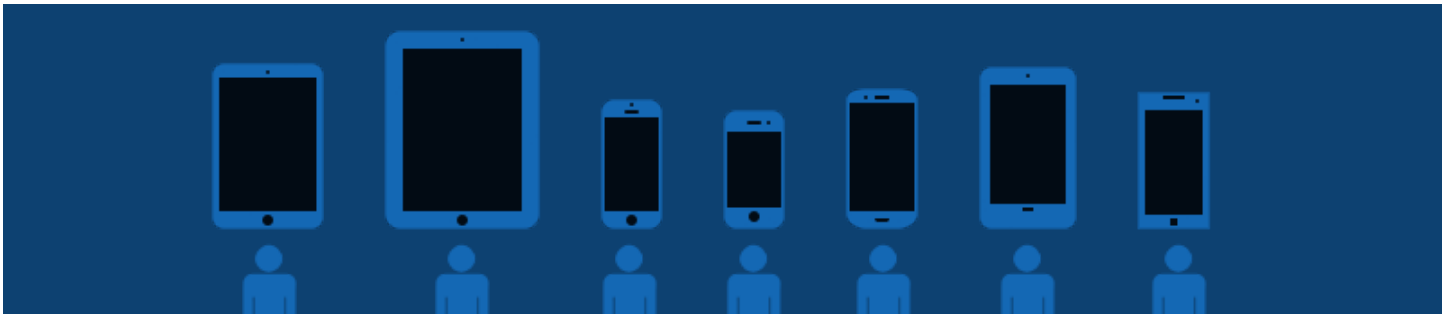
24%

of surveyed consumers use personal devices to handle work-related computing

IF YOU'RE CONSIDERING BYOD...

To begin, we'll take a quick look at the facts:

- 89% of employees access business applications from outside the office
- BYOD will grow to 350 million users by the end of 2014
- 95% of companies currently allow their employees to use personal devices for work purposes
- More than 75% of employees believe that having a single device helps balance their work and personal lives



Companies pursue BYOD policies for many different reasons. The primary benefits of a BYOD strategy include:

- Increased productivity through an employee's familiarity with their own mobile device. As opposed to having to learn how to work with a new device, BYOD policies capitalize on an employee's existing knowledge and workflow.
- Higher employee satisfaction by allowing for the greatest degree of personalization and customization while handling company business
- Reduced platform dependence By organizing IT infrastructure to adapt to a number of different operating systems and devices, a BYOD plan ensures that the company does not become locked into longterm dependence on a particular software or device vendor.
- Potential cost savings trhrough eliminating the purchase of company specific devices, IT resources can be better utilized to serve the needs of existing devices and users without having to invest in hardware, software, setup and training.

THE BENEFIT OF CUSTOM APP SOLUTIONS

BYOD allows companies greater control over tailoring their user experience, making their infrastructure employeefocused, resulting in greater productivity and satisfaction within the work environment. As opposed to wrestling with existing apps that may not do everything employees need, BYOD allows for companies to invest in the software that will get the job done.

The nature of BYOD policies means that two or more operating systems will be used across the workforce. When building an app for a BYOD environment, it may be tempting to try an "all in one" solution that works on iOS, Android, and other platforms. These kinds of apps are called "crossplatform" apps; their counterparts that are developed for only one platform are called "native" apps. With this in mind, it's important to acknowledge the differences between native and crossplatform app development.

Native development that is, creating an app written in the platform's native programming language is an essential part of creating an effective and secure BYOD app. Although crossplatform apps may promise savings in cost and frustration, platform updates and devices changes can quickly render them obsolete and ineffective. Conversely, natively developed apps will work with greater reliability and adaptability to your BYOD users. When making an app for a BYOD environment, it is worth every penny to develop the app natively for each platform in use.

The primary caveat with native development is the cost of developing a separate application for each platform, particularly for platforms that aren't as widely used as iOS and Android. When considering a BYOD policy, it's essential to consider the possibility of an employee who refuses to give up their Blackberry. They'll need to be able to access company apps just as much as their iOS and Android peers, and the IT department will have to respond accordingly.

In the same sense that BYOD allows for employees to use a custom solution that works for them, BYODfocused apps allow companies to develop software solutions that best serve their needs.

SECURITY

BYOD may seem riskier in terms of information security in truth, it was a much more hazardous policy to follow before the popularization of powerful smartphones. That being said, every company with a stake in the mobile device industry has made efforts to improve the security features of their product, from the device manufacturer to the carrier network and every company in between.

89%

of employees access business applications from outside the office

Security is as much a concern in BYOD as in any other IT policy. In a broader sense, a BYOD plan poses unique security problems, such as ensuring that proprietary information is kept on company servers, and that access to this information is removed when employees leave the company.

As smartphone usage has grown in the workplace, IT security tools have consequently grown and adapted to this influx of devices. Some of the most critical tools used by BYOD IT departments are known as mobile device managers (MDMs). Through MDMs, IT departments now have the ability to control read/write permissions, file downloads, and server authentications on mobile devices despite not having actual physical control over the device.

A number of different MDMs are available in the marketplace, including VMWare's AirWatch, IBM's MaaS360, MobileIron, and Excitor. Although each offers its own unique advantages and disadvantages, MDMs generally allow for a company to:

- Monitor a device's location and data use
- Safeguard data and transmissions through existing company security certifications Control access to servers, email, and calendar information
- Install, update, repair, and remove companyowned applications from the device
- Remotely wipe data from lost, stolen, or partiallydestroyed mobile devices

In some cases, it may be much easier to secure a BYOD workforce than to secure a group of employees carrying companyowned devices. Since the employees own the phones and tablets, they have a vested interest in maintaining the physical security of the device itself, allowing the IT department to focus solely on controlling what information the device can access.

Ultimately, a BYOD policy is no more or less hazardous for information security than any other kind of technology plan. As with any kind of company policy, BYOD requires planning, consulting, and an understanding of the needs of the workforce.

77% of employees haven't been educated about the security risks of BYOD.

INTERNATIONAL ISSUES

As any IT director can testify, the culture and working styles of teams can vary immensely from office to office and nation to nation. That said, BYOD strategies are still a viable option for companies with multinational operations; however, implementing such a strategy across the entire company requires diligent cooperation between IT directors who may not share a common language or technological familiarity. When considering an international BYOD policy, it's important to keep certain potential problems in mind, such as:

- Device and software availability Instantaneous global launches of devices are rare; indeed, the iPhone 5's release was staggered over the course of three months. Accordingly, BYOD policies must account for the fact that not all employees will be able to access the latest device and software iterations.
- Cultural acceptance although BYOD is relatively wellestablished in the United States, the cultures of other nations may not be as receptive to the idea of having a "work device" on one's person at all times, even if it's also used for personal matters.
- Operating system popularity Android and iOS are very firmly established

as the two primary mobile operating systems for American workers. However, different countries may boast large groups of employees using Windows Phone, Blackberry, and other platforms, increasing the potential development cost for company apps.

- Maintenance Planning, coordinating, and implementing maintenance across multiple time zones is an immense undertaking, and must be accounted for when considering a BYOD approach
- Legality National and local governments may have differing regulations on how workrelated technology can be used, apportioned, and funded.

Presently, it would appear that BYOD is more popular in the United States than Europe, in part because European employees expect their employers to provide their work devices. Despite this, BYOD may still be a viable option for companies with European offices, particularly as it continues to become more widely adopted in the States.

Like any company policy, it's important to discuss a BYOD plan with every relevant department, including IT, marketing, legal, and the management for each region that will be affected by the plan.

HARDWARE COSTS/MAKING THE DECISION

One of the most significant benefits to a BYOD policy is hardware cost which is to say that there really isn't much of one. If the employee elects to own the device, they can reasonably be expected to cover the full cost of the device themselves. There are cases where an employee can receive a stipend for a portion of the cost of the device if they stay with the company for a certain period of time after the purchase; however, these policies can vary widely from company to company.

In looking at the larger implications of BYOD, the single largest caveat in letting employees purchase the device could be the inclination to go for the absolute lowest cost possible. This could result in employees handling company matters from devices and operating systems that are no longer supported by the device manufacturer, making it that much more difficult for the employee to do their job and for the IT team to support the device. With this in mind, it is essential for employers to stipulate that if employees choose to enroll in a BYOD plan that they must purchase a device of a generation that will be usable for the next three to five years. This ultimately translates into cost savings for both the employee and employer.

WHAT ABOUT TABLETS?

Although BYOD strategies tend to largely focus on smartphones, many companies must also allow for the fact that their employees will use tablets to handle work-related functions. As Android tablets have not yet been widely adopted for business purposes, it is safe to assume that all tablets in a company's workforce will be iPads.

Mobile phones **AND** tablets are both experiencing growths in usage at the workplace

Tablets are just as easily managed as any other mobile device in a BYOD plan; the only difference is that custombuilt applications must account for the differences between tablets and their mobile phone kindred. The idea of scalability comes to mind that is, that a custom BYOD app must be able to respond to the dimensional and operational differences across every device that may support it. It's also essential to consider the data needs of tablets; if employees must access corporate data from the field, will they have mobile data plans, or will a WiFi connection be necessary?

POTENTIAL RISKS AND ARGUMENTS AGAINST

Despite the growing popularity of BYOD movements, many companies elect to go with traditional IT plans for a number of reasons. It's certainly true that companies have greater control over employee devices if said devices are companyowned; additionally, there are certain cost reductions that come with providing devices of a single platform. These savings come in the form of a simplified planning process, unified technical support, and the need to only develop applications for one operating system. However, companypurchased devices will need to be upgraded every three to five years in order to stay current with ongoing technology trends, which may overwhelm the initial cost savings.

CONCLUSION

Like any IT strategy, the feasibility and practicality of BYOD depends largely on the culture and mission of your company. Employees and managers alike should be consulted before moving forward with any concrete implementation of a BYOD plan so that the needs of the users and the company alike can be duly served. When done properly, a BYOD can offer immense benefits in terms of cost, productivity, security, and adaptability.

About Accella

We specialize in creating happy clients through the design, development, and promotion of websites and mobile applications.